(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 44 16 595 A 1**

(51) Int. Cl.[6]:
**H 04 L 9/32**
H 04 L 9/14

(21) Aktenzeichen: P 44 16 595.1
(22) Anmeldetag: 11. 5. 94
(43) Offenlegungstag: 16. 11. 95

DE 44 16 595 A 1

(71) Anmelder:
Deutsche Bundespost Telekom, 53175 Bonn, DE

(72) Erfinder:
Stolz, Helmut, Dipl.-Ing., 57080 Siegen, DE;
Kowalski, Bernd, Dipl.-Ing., 57072 Siegen, DE; Bothe, Heinz-Jürgen, Dipl.-Ing., 63329 Egelsbach, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

| | |
|---|---|
| DE | 39 19 734 C1 |
| EP | 1 48 960 A1 |
| SU | 17 85 577 A3 |

(54) Verfahren zur Sicherung von verschlüsselten vertraulichen Informationsübertragungen

(57) Bei der Informationsübertragung von Signalisierungs-, Steuerungs- und Überwachungsinformationen bestehen Sicherheitsprobleme, um Beeinflussungen, Abhören, Manipulationen Dritter und Fehlinterpretationen sicher zu vermeiden.
Die Erfindung löst diese Problematik durch Ersatz der Systemkennungen durch Zertifikate, wobei die Module über Sicherheitseinrichtungen der Zentrale und der Außenstellen in wechselweise Verbindung, zunächst zur Urinitilisierung mit sitzungsindividueller Authentikation, treten, wonach eine zugriffssichere Speicherung einer ID und eines Zeitregimes für ISDN-Rufnummer und UUS-frame Sendungen durchgeführt werden.
Anwendungsgebiete der Erfindung sind vertrauliche verschlüsselte Informationsübertragungen aller Art.

DE 44 16 595 A 1



Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 09. 95 508 046/181

Beschreibung

Die Erfindung bezieht sich auf ein Verfahren der im Oberbegriff des Patentanspruches 1 näher definierten Art. Ein derartiges Verfahren ist z. B. in DIN ETS 300 100-1 "ISDN usre network interface layer 3 specification for Basic call control", in DIN ETS 300 100-2 "ISDN user network interface layer 3 specification for Basic call control-SDL", sowie im Document No.: T/S 46-33T version 5, Date: 1991-12-06 "USER to USER signalling (UUS) Sapplementary service" von ETSI beschrieben.

Die bekannten Lösungen weisen einen entscheidenden Mangel auf: die Beeinflussungsmöglichkeit des Gesamtsystems durch gezielte Angriffe und damit Schwächung der Funktionalitäten "Steuern, Regeln, Überwachen".

Bei den bekannten Lösungen/Systemen können die Nachrichteninhalte (hier im UUS) auf dem Übertragungsweg von Angreifern beeinflußt und/oder abgehört werden. Außerdem könnten Angreifer gezielte Falschinformation einspielen und damit die Integrität angreifen. Dies würde zu Fehlinterpretationen führen und die Gesamtfunktionalität des Systems in Frage stellen. Der Systembetreiber würde mit unnötigen Kosten belastet.

Bei Nutzung des UUS zum Transport von Signalisierungs-, Steuerungs- und Überwachungsinformationen in einem offenen Kommunikationssystem, hier EURO-ISDN, besteht die Gefahr, daß unberechtigte Personen und nicht autorisierte Systeme bzw. Systemkomponenten die Informationsinhalte im UUS manipulieren und/oder abhören können. Die Aussagekraft des Gesamtsystems wird damit in Frage gestellt, und die Zuverlässigkeit ist nicht gegeben.

Aus diesem Grunde sind, als Aufgabe der Erfindung, durch eine Veränderung der Verfahrensweise geeignete Sicherheitsvorkehrungen zu treffen.

Diese Aufgabe wird durch die im Kennzeichen des Patentanspruch 1 aufgeführten Verfahrensschritte gelöst.

Vorteilhafte Weiterbildungen des Verfahrens sind in den Kennzeichen der Ansprüche 2 bis 4 beschrieben.

Es ist dabei das Prinzip der Erfindung, die Systemkennungen (der entspr. Equipments in den Außenstellen und Betriebszentralen) sowie eventuell vorhandene Operatorpaßworte, die zur Identifizierung der in den Außenstellen- und Betriebszentralen benutzten Equipments und ggf. Operator dienen, durch sogenannte Zertifikate zu ersetzen.

Moderne Zugangssicherungs- und Kommunikationssicherungsverfahren erlauben den Einsatzchipkarten- und sicherheitsmodulgestützter Verfahren. Sie können beliebig lange und beliebig komplexe "Paßworte" auch Systemkennungen (quasi Systemidentitäten) speichern. Sicherung gegen Ausforschung durch Verwendung von Chipkarten und chipkartengestützten Sicherheitsmodulen in entsprechenden Sicherheitszusatzeinrichtungen mit EUR0-ISDN Schnittstellen.

Die Erfindung wird nachstehend an Ausführungsbeispielen näher erläutert:

Bestandteile der Zertifikate:

- Identität (Name) des Equipments der Außenstelle und Betriebszentrale sowie ggf. des Operators
- Ausgabedatum und Gültigkeitsdatum
- Ausgabestelle (Name)
- öffentlicher, personalisierter Schlüssel des in Außenstellen und Betriebszentralen vorhandenen Equipments sowie des Operators
- die, durch den geheimen Schlüssel der Ausgabestelle kryptographisch gesicherte elektronische Unterschrift aller im Zertifikat enthaltenen Daten unter Verwendung eines public key Kryptoverfahrens.

Weiter werden die Nachrichteninhalte im UUS mit authentisch übermittelten "Sitzungsschlüsseln" zwischen den Außenstellen und Betriebs zentralen verschlüsselt und somit gegen Angriffe geschützt.

Erläuterung des authentisch übermittelten Sitzungsschlüssels.

Betriebszentrale und Außenstelle führen eine sitzungsindividuelle Authentikatifikation (z. B. nach dem challenge und response Verfahren) unter Verwendung ihrer geheimen "System-Schlüssel" durch; dabei generiert einer der beteiligten Equipments einen Sitzungsschlüssel (symmetrischer Schlüssel) und sendet ihn als verschlüsselte Information dem anderen Equipment unter Verwendung dessen öffentlichen Schlüssels.

Es obliegt der Betriebszentrale bzw. dem Operating, wie lange (Zeitraum) ein authentisch übermittelter Sitzungsschlüssel zwischen der Betriebszentrale und einer Außenstelle benutzt wird.

Entsprechend den Einstellungen des Operatings (Zeitintervall für Nutzung des gleichen Schlüssels) generiert die Sicherheitsrichtung der Betriebszentrale einen neuen Verschlüsselungsschlüssel und überträgt diesen mit einem entspr. Befehl im UUS zur Außenstelle. Damit ist sichergestellt, daß in einstellbaren Zeitintervallen andere Schlüssel benutzt werden.

Der Funktionsablauf ist unter den Voraussetzungen:

- Installation der Sicherheitseinrichtung in der/den Betriebszentrale/n und Eingabe der ISDN-Rufnummer der Außenstellen,
- Funktionsfähiger ISDN-Anschluß,
- Installation der Sicherheitseinrichtung in den Außenstellen und Eingabe der ISDN-Rufnummer der zuständigen Betriebszentrale/n und
- Funktionsfähiger ISDN-Anschluß,

wie folgt zu erklären:

Nach Installation der Sicherheitseinrichtung in der Außenstelle und Eingabe der ISDN-Rufnummer der Betriebszentrale wird automatisch oder manuell eine Verbindung (Aufruf für Urinitialisierung) vom "Modul" über die Sicherheitseinrichtung zur Betriebszentrale angefordert. (Interne Nutzung der UUS zwischen Modul und Sicherheitseinrichtung).

Die Sicherheitseinrichtung der Außenstelle baut nun eine Verbindung (im EURO-ISDN) zur Sicherheitseinrichtung in der Betriebszentrale auf und fordert einen B-Kanal für Datenübertragung an.

Die beiden Sicherheitseinrichtungen vereinbaren eine "Urinitialisierung für Außenstelle". Danach erfolgt eine gegenseitige sitzungsindividuelle Authentikation, Generierung eines "Sitzungsschlüssels" und authentische und vertrauliche Übertragung desselben zur Außenstelle.

Der Sitzungsschlüssel wird in den Sicherheitsmodulen für UUS Nutzung unausforschbar gespeichert. Danach wird die Verbindung abgebaut und der B-Kanal kann für andere Anwendungen benutzt werden.

Zusätzlich kann die Sicherheitseinrichtung SEZ in der Zentrale eine Außenstellen- ID generieren und als ver-

trauliche Info der Außenstelle senden und intern speichern. In diesem Fall würde die SE der Außenstelle diese ID speichern und als def. UUS Info an das Modul weitergeben.

Immer, wenn das Modul einen Befehl oder eine Meldung an die SE sendet, wird die ID des Moduls mit der ID in der SE überprüft.

Die SEZ in der Betriebszentrale sendet eine Information an die zentrale Einrichtung. Applikation zur Außenstelle (ISDN-Rufnummer) kann genutzt werden (ggf. wird die ID mit übertragen).

Die zentrale Einrichtung reiht die Außenstelle in die Abrufliste ein (ggf. wird TD-Außenstelle in entspr. Rechtedatei aufgenommen).

Die SEZ ergänzt ihre gesicherte zugriffsgeschützte Datei — ISDN-Rufnummer/akt. Schlüssel und überwacht den "Generierungszeitpunkt-Schlüssel".

Sobald die zentrale Einrichtung aufgrund der internen Abrufliste (zeitgesteuert) eine Außenstelle ansprechen will, sendet sie die ISDN-Rufnummer der Außenstelle und das entspr. Infofeld als UUS Info an ihre SEZ. Diese holt den entspr. Sitzungsschlüssel und verschlüsselt den UUS-Frame bzw. Teile des UUS-Frames und sendet dies ins Netz.

Die SEA der Außenstelle entschlüsselt den UUS-Frame, sendet ihn zum Modul. Das Modul wertet aus und sendet als Antwort UUS-Frame (evtl. mit ID) und ISDN-Rufnummer der Zentrale an SEZ.

Die SEA verschlüsselt UUS-Frame bzw. Frameteile und sendet ISDN-Rufnummer und UUS-Frame zum Netz.

SEZ Zentrale entschlüsselt UUS-FRame und gibt ihn an die zentrale Einrichtung weiter. Diese wertet aus und veranlaßt weiteres.

Wichtig: Nach Empfang UUS von Außenstelle auf Anforderung durch Zentrale erfolgt kein Aufbau des B-Kanals.

Die Außenstelle kann ebenfalls zwischen 2 Abfragen Events/Alarme an die Zentrale melden.

Sie sendet die ISDN-Rufnummer der Zentrale und UUS-Frame an die SEA. Diese verschlüsselt den UUS-Frame oder Teile und sendet die Info ins Netz. Die zentrale SEZ entschlüsselt UUS und gibt Frame an die zentrale Einrichtung. Diese wertet aus und sendet entsprechend Frame an SEZ. Diese sendet nach Verschlüsselung UUS-Frame an Außenstelle.

In gewissen Zeitabständen ist ein Sitzungsschlüsselwechsel erforderlich.

Zwei Alternativen sind vorstellbar:

1. SEZ in der Zentrale überwacht Generierungszeit und generiert nach deren Ablauf einen neuen key. Diesen sendet sie verschlüsselt auf den alten key der SEA einer Außenstelle.
2. Gleiches Verfahren wie bei Urinitialisierung, jedoch mit dem Hinweis "Schlüsselwechsel".

## Patentansprüche

1. Verfahren zur Sicherung von verschlüsselten vertraulichen Informationsübertragungen in offenen Kommunikationssystemen zwischen Außenstellen bzw.
Zentralen mit Modul, insbesondere von Signalisierungs-, Steuerungs- und Überwachungs-Informationen im user-user signalling (UUS) des D-Channel (D-Kanal) des Pan European Integrated Services Digital Network (ISDN) (In Deutschland EURO-ISDN), **dadurch gekennzeichnet,** daß nach der Installation einer Sicherheitseinrichtung (SEA) in der Außenstelle und Eingabe der ISDN-Rufnummer zuerst vom Modul eine Verbindung über die Sicherheitseinrichtung (SEA) zur Zentrale zwecks Urinitialisierung angefordert wird, die von der Sicherheitseinrichtung der Außenstelle (SEA) dann zur Sicherheitseinrichtung der der Zentrale (SEZ) (bzw. später zwecks Schlüsselwechsel auch in umgekehrter Richtung) mit Anforderung eines B-Kanals für Datenübertragung aufgebaut wird, daß danach eine gegenseitige sitzungsindividuelle Authentikation mit Generierung und authentischer und vertraulicher Übertragung eines Sitzungsschlüssels von der Zentrale zur Außenstelle durchgeführt wird, wo dieser als UUS-frame (Rahmen) unausforschbar für die UUS-Nutzung gespeichert wird, daß danach die Außenstelle in eine gesicherte zugriffsgeschützte Abrufliste der Zentrale eine Identifizierung (ID) mit ISDN-Rufnummer und Schlüssel für zeitgesteuerten Abruf gespeichert und diese erste B-Kanal-Verbindung aufgelöst wird und daß danach, bei erneuten Verbindungen (zeitgesteuert von SEZ zu SEA bzw. bei Events/Alarmmeldungen von SEA zu SEZ), jeweils die ISDN-Rufnummer und UUS-frame gesendet werden, wonach die Gegenstelle wenigstens teilweise den UUS-frame mit dem aktuellen Sitzungsschlüssel verschlüsselt und über das Netz zur rufenden Stelle sendet, welche UUS-frame entschlüsselt, zum Modul zur Auswertung sendet und als Antwort wieder UUS-frame und ISDN-Rufnummer sendet.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der spätere Schlüsselwechsel nach Ablauf eines festgelegten Zeitlimits mittels einer erneuten sitzungsindividuellen Authentikation mit Generierung und authentischer und vertraulicher Sitzungsschlüsselübertragung durchgeführt wird.
3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Schlüsselwechsel im UUS-frame (Rahmen) unter Nutzung eines vertraulichen neuen Sitzungsschlüssels (S-key) durchgeführt wird.
4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß durch die Sicherheiteinrichtung der Zentrale (SEZ) eine Identifizierung (ID) generiert, als vertrauliche Information an die Außenstelle gesendet, und intern (SEZ) und in der Sicherheitseinrichtung der Außenstelle (SEA) gespeichert und dem UUS-frame zugesetzt wird.

– Leerseite –